Addressing the incremental risks associated with adopting a Bring Your Own Device program by using the COBIT 5 framework to identify key controls.

by
Lyle Weber

Thesis presented in fulfilment of the requirements for the degree of MCOMM (Computer Auditing) in the Faculty of Economic and Management Sciences School of Accounting at Stellenbosch University

Supervisor: Mrs Sybil Smit
Co-supervisor: Professor Willie Boshoff

April 2014

Declaration

By submitting this thesis electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by Stellenbosch University will not infringe any third party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

December 2013

ACKNOWLEDGEMENTS

I want to thank GOD the FATHER for HIS LOVE, My LORD and SAVIOUR JESUS CHRIST for being a great example and the HOLY SPIRIT who greatly assisted and guided me with during the course of the research.

I would also like to thank my dad (Gavin Weber), my mom (Glenda Weber) and my two sisters (Jamie-Leigh Weber and Kayla Chandre' Weber) for their continuous love, support and encouragement.

Finally I would like to thank my supervisor Ms. Sybil Smits for her guidance throughout the process and continuous words of encouragement too.

ABSTRACT

Bring Your Own Device (BYOD) is a technological trend which individuals of all ages are embracing. BYOD involves an employee of an organisation using their own mobile devices to access their organisations network. Several incremental risks will arise as a result of adoption of a BYOD program by an organisation. The research aims to assist organisations to identify what incremental risks they could potentially encounter if they adopt a BYOD program and how they can use a framework like COBIT 5 in order to reduce the incremental risks to an acceptable level. By means of an extensive literature review the study revealed 50 incremental risks which arise as a result of the adoption of a BYOD program. COBIT 5 was identified as the most appropriate framework which could be used to map the incremental risks against. Possible safeguards were identified from the mapping process which would reduce the incremental risks to an acceptable level. It was identified that 13 of the 37 COBIT 5 processes were applicable for the study.

Contents

List of Tables

CHAPTER 1: INTRODUCTION

1.1 Background

What started out several years ago with individuals using their own personal computers to access their organisations networks via dial up and virtual private networks has changed dramatically in recent years.

There has been an extensive rise in the number of smart phone and tablet computer sales in recent years. Gupta, A. et al (2013) indicated that global smartphone sales reached 225 million units in the second quarter of 2013. Deloitte (2013) indicated that there are over 10 million active smartphones in South Africa.

With the increased number of smartphone and tablet computers circulating in the market place, it comes as no surprise that more and more individuals are making use of their personal mobile devices to connect to their organisations networks. Whilst there are benefits which the organisation derives such as cost saving and happier employees - which results in increased productivity, there are incremental risks which arise as well. The concept where an employee uses his/her own personal mobile device to connect to the organisation's network is known as Bring Your Own Device (BYOD).

BYOD has been embraced by a large number of organisations of various sizes and in various sectors.

Some employees use their mobile devices to perform basic tasks such as syncing their work emails and calendars with their mobile devices, whereas other employees use their mobile devices to perform specific work related tasks such as compiling Excel spread sheets and accessing sensitive corporate data.

Failure on the behalf of the organisation to implement sound internal controls and governance policies to address the risks associated with BYOD could lead to the organisation suffering dire consequences. These consequences include, but are not limited to:

- heavy financial losses, and
- the risk of potentially closing down, If
    - if sensitive client data is leaked into the public arena as a result of data theft, or
    - where malware infiltrates the network and corrupts the data or causes the information technology system to shut down.

The governance of the incremental risks should not only be of interest to those charged with governance of the organisation, but to the external auditor as well. The auditor would need to understand which incremental risks have arisen as a result of the adoption of the BYOD program. Failure to adequately identify these incremental risks could result in the auditor expressing an inappropriate audit opinion.

Most of the research conducted to date on BYOD programs looks at the benefits of adopting such programs and to a lesser extent, the incremental risks associated with the implementation of BYOD programs.

This research will therefore produce valuable information for organisations wishing to adopt a BYOD program, organisations that currently run BYOD programs and external auditors.

1.2 Problem statement

An organisation that adopts or deploys a BYOD program will be faced with increased incremental information technology strategic and operational risks. These organisations will need to identify suitable internal controls in order to reduce the incremental risks to an acceptable level.

1.3 Objective

The objective of this study is to develop a framework to identify and manage the incremental information technology strategic and operational risks which arise when an organisation adopts a BYOD program.

The study will focus mainly on the incremental strategic risks which arise as a result of the adoption of a BYOD program and to a lesser extent on the incremental operational risks which arise when an organisation adopts a BYOD program.

1.4 Scope of the research

It is not the purpose of this research to identify all the incremental risks that an organisation will encounter as a result of adopting or deploying a BYOD program, neither the identification of all the controls and safeguards which an organisation could adopt to reduce the incremental risks to an acceptable level.

The research is also limited to information technology strategic and operational incremental risks which arise when adopting a BYOD program.

1.5 Research motivation

Most research relating to BYOD has been conducted by private organisations such as IBM, Gartner, ISACA and Forrester.

The benefits arising from BYOD have been widely researched, as documented by some, including Pelino (2012); DAT (2012) and Anderson

(2013). However only a limited amount of research has been conducted to date on the risks and concerns which arise when an organisation adopts a BYOD program. Rose's (2012) article indicates that there are security implications which arise as a result of BYOD. Markelj and Bernik's (2012) article indicates the threats that arise as a result of using mobile devices and the impact on corporate data security.

A practical integrated framework will assist those charged with governance at the organisation in mitigating the risks associated with the adoption and deployment of a BYOD program to an acceptable level.

The findings of the research conducted may be used as a guideline in assessing the incremental information technology strategic and operational risks which may exist at the organisation as a result of the organisation adopting a BYOD program. The findings may also be used to identify key controls that could be deployed to reduce the incremental risks to an acceptable level.

1.6 Organisation of the research

The dissertation will consist of the following chapters:

Chapter 2: Research methodology: A comprehensive literature review was performed and a practical integrated framework was developed based on the findings of the literature review.

Chapter 3: Literature review: An extensive literature review was conducted to identify the incremental information technology strategic and operational risks which arise as a result of an organisation adopting a BYOD program.

Chapter 4: Selection of control framework: Motivation for the selection of COBIT 5 as the framework to be used in this study.

Chapter 5: Findings on the incremental information technology strategic and operational risks which arise when an organisation adopts a BYOD

program: Incremental risks identified during the study were mapped against possible controls and safeguards to reduce the risks to an acceptable level.

Chapter 6: Conclusion: This chapter contains an overview of the research, highlighting the outcomes of the research findings and discusses future research to be conducted.

CHAPTER 2: RESEARCH METHODOLOGY

2.1 Purpose of the study

The aim of this study is to identify key internal controls and safeguards which an organisation can deploy by using the COBIT 5 framework as a basis to reduce the information technology strategic and operational risks identified to an acceptable level. The study is non-empirical in nature and the results drawn are from an extensive literature review.

2.2 Literature study

An extensive literature review was performed on BYOD and the COBIT 5 framework.

The following considerations highlight some of the key areas focused on during the literature review:

- Risks and concerns relating to BYOD programs,
- Compliance and legal considerations which arise as a result of BYOD,
- The behaviour of employees whilst using their own devices,
- Implications of mobile devices being stolen or lost, and
- The COBIT 5 framework.

2.3 Research methodology

In order to identify the key internal controls needed by an organisation to reduce the incremental information technology strategic and operational risks which arise as a result of an organisation adopting a BYOD program to an acceptable level, the following steps were taken:

Step 1: Conduct an extensive literature review on BYOD.

Step 2: The incremental information technology strategic and operational risks were summarised in tabular format.

Step 3: Select a control framework.

Step 4: Identified which COBIT 5 processes were applicable for the purpose of this study.

Step 5: Mapping of COBIT 5 to the risks identified during the extensive literature review was tabularised.

Step 6: Possible safeguards or controls for the incremental information technology strategic and operational risks identified in step 2 were summarised in tabular format.

2.4 Conclusion

By implementing the above-mentioned methodology at both a strategic and an operational level, it will be shown that compliance with IT governance principles is possible at both the strategic and operational levels.

CHAPTER 3: LITERATURE REVIEW

3.1 BYOD

Mobile devices (USB's, tablet computers, laptops, smartphones) of all shapes and sizes have become a part of our daily lives.

The concept of BYOD (Bring Your Own Device) involves permitting an employee to connect their own personal mobile devices to the organisations network and applications. The BYOD concept has been adopted by organisations, both governmental and non-governmental of all sizes and across all industries (Burt, 2011; Gatewood, 2012; Willis, 2013b).

Gupta, A. et al (2013) indicated that smartphone sales to end users have reached 225 million units in the second quarter of 2013 and Rohan (2013) stated that employees are using their personal mobile devices for official work purposes.

If organisations do not support employees in their wish to use their own personal devices for work purposes, the employees may figure out ways to support their devices themselves. This will place sensitive corporate data at risk. It is therefore important that organisations enable employees to get their work done in the most appropriate manner without compromising the integrity of the data. (Kanaracus, 2012)

Whilst it is not the purpose of this paper to discuss the benefits associated with the adoption or deployment of a BYOD program, a few benefits are listed. The benefits include, but are not limited to:

- Increase in productivity of employees (Pelino, 2012; (DAT, 2012), 2012; Anderson, 2013)
- Increased revenue (Pelino, 2012); and
- Reduction in expenses for corporate-liable mobile device and data services (Pelino, 2012; DAT, 2012).

Based on the abovementioned benefits it is understandable why many organisations would be inclined to opt for the adoption and deployment of BYOD programs. It should however be noted that whilst the benefits are good, failure to consider the concerns and risks surrounding the adoption or deployment of a BYOD program noted by industry experts, could have dire consequences on the organisation.

Several concerns and risks were identified during the extensive literature review that was conducted. The concerns and risks identified arise as a result of an organisation deploying a BYOD program. These concerns and risks indentified have been classified as either strategic or operational in nature and have been discussed below in section 3.2 and 3.3.

3.2 Strategic incremental concerns and risks

3.2.1 Malware

Malware enables hackers to steal passwords and in some cases even creates an opportunity for the hacker to take control of the organisations computer systems, including those that run smartphones and tablets (Staut, 2012).

With the BYOD concept being adopted on an increased basis by organisations across all business sectors, it comes as no surprise that many organisations are increasingly being affected by malware. This is due to the fact that there has been an increase in the amount of new malicious smartphone and tablet targeting software (Drew, 2012; Kaspersky, 2012; Ponemon Institute LLC, 2012; Lung Kao, 2011).

The Ponemon Institute LLC (2012) indicated that traditional security solutions which most organisations employ, such as antivirus, firewalls, and passwords are not effective at stopping malicious or negligent employees of the organisation from deploying advanced malware into the organisations computer systems.

Users who access the Internet from their mobile devices are at constant risk of exposure to web-based threats, including data stealing malware. When a device downloads a new mobile application from any online application store, the software may contain malware that can steal or damage data on the device and, in some cases, even disable the mobile device itself (CISCO, 2013).

According to the Cisco survey results, 69% of BYOD users were using unapproved applications on their devices, which is difficult to detect (Cisco, cited in DAT, 2012). The recent staggering increase in Android malware magnifies this problem (DAT, 2012).

If an organisation fails to have proper internal controls in place to manage the risks associated with malware, the organisation could find itself being the target of some or other malicious malware attack which could have a disastrous impact on the organisation.

3.2.2 Data leakage

Each organisation has different types of data which they deal with on a daily basis. Some data types are more sensitive than others, e.g. documents containing trade secrets or confidential client information would be more important than the organisations policy on whistle blowing. The risks associated with data leakage on mobile platforms have become a bigger problem than malware (Willis, 2013b).

It is for this reason that organisations should be interested in safeguarding their data in order to prevent unauthorised individuals from gaining access to what could be seen as their most important asset.

If an organisation has deployed a BYOD program, there is a high probability that employees will sync their mobile devices with their home computers. This increases the risk of data leakage as the employee's home computer may already be infected with malware such as Trojan horses and spyware which would compromise the security of corporate data. If the employee's home computer has any unpatched vulnerabilities, this will grant cybercriminals the ability to gain access to the mobile data that has been backed up, stored or synced onto the employee's home computer (Kaspersky, 2012).

Willis, (2013b) stated that most mobile devices are designed to share data via the cloud. Rouse, (2010) indicates that cloud computing involves delivering hosted services over the internet. Whilst Cloud based sharing and storage of personal data is convenient, employees may forward sensitive documents and presentations relating to the organisation to their personal email like Google Mail or file storage services like Dropbox so that they can access the information on their mobile device at a later stage. This would create a "shadow infrastructure" over which the organisation will have little to no control and will result in a direct increase in the risk of data leakage taking place (Anderson, 2013; IBM, 2011).

The Ponemon Institute found the average organizational cost of a data breach increased to US$7.2 million and cost companies an average of US$214 per compromised record (IBM, 2012).

Failure on behalf of an organisation to safeguard their data through the implementation of proper internal controls could result in the organisation not only suffering legal action and huge financial losses, but depending on the extent of the breach, could cause irreparable damage on the organisations ability to continue in the future.

3.2.3 Theft or loss of mobile devices

Mobile devices are popular amongst individuals of all ages. These devices are generally compact in nature, yet they have the ability to be used to perform similar tasks to most personal computers. It should come as no surprise that in a report prepared by IBM (2011) as well as research conducted by Markelj and Bernik (2012), that the most frequently seen mobile device security threats are the loss and the theft of these devices.

The loss of a personal smartphone or tablet on which an employee has downloaded confidential data of the organisation, creates an opportunity for a criminal to access the organisations confidential information. This represents a serious security risk for the organisation (Kaspersky, 2012). This is especially the case where the employee has not followed basic security practises such as locking the device with a strong password and encrypting sensitive data transmitted to and from the mobile device (Staut, 2012).

Mobile data-bearing devices that were lost or stolen may contain sensitive or confidential information (Ponemon Institute LLC, 2012; Drew, 2012). The data stored on the device may be compromised if access to the device or the data is not effectively controlled (Evangelista, 2013). The risk of unauthorised access to the data is further increased as most organisations do not have the ability to remotely wipe a device if a smartphone is lost or stolen. Most employees do not know what to do if their device was lost or stolen (Rose, 2012).

It is for this reason that users of mobile devices need to take some form of precautionary measure to ensure that they too do not form part of the population of individuals who have lost their mobile device or have had it stolen from them.

3.2.4 Connectivity of the device (Bluetooth and Wi-Fi)

Mobile devices offer broad Internet and network connectivity through varying channels including, but not limited to Bluetooth and Wi-Fi technology.

Anderson (2013) stated that when an authenticated device has other devices tethered to it, it may be possible for non-authenticated devices and users to gain access to the corporate network by connecting through the authenticated device. The threat to the corporate network is further increased as Bluetooth

and Wi-Fi technology can be easily exploited to infect a mobile device with malware or compromise transmitted data (IBM, 2011).

When a Bluetooth device is set on discoverable mode, it makes it very easy to scan for the device using a computer. Once the computer is connected to the device the computer is able to download the private data located on the device (Cisco, 2013).

Users who make use of Bluetooth and Wi-Fi technology to connect to the Internet or to share information should be mindful that these channels may not be as safe as what they may have originally thought.

3.2.5 Web based applications

Web based applications are quite often designed by individuals who the owner of the mobile device may not know personally. Mobile device users normally download applications which are of interest to them onto their mobile devices.

There are more than 700 000 apps in the Apple App Store and more than 700 000 apps in the Android Marketplace (Tibken, 2012).

When a device downloads a new mobile application from any online application store, the software may contain malware that can steal or damage data on the device and, in some cases, even disable the mobile device itself. It is not possible for application store owners to conduct in-depth code reviews of all applications (IBM, 2012; IBM, 2011). Anderson (2013) indicated that individuals are more than likely to use their personal mobile devices to access both personal and business applications.

An IBM survey conducted on several hundred of their employees revealed that many of their employees were completely unaware which popular apps were security risks (Rose, 2012). The risks are further increased by the recent staggering increase in Android malware (DAT, 2012).

Web based applications can therefore cause a substantial amount of damage to the organisations IT infrastructure if the use of these applications are not properly controlled.

3.2.6 Compliance with laws and regulations governing the organisation

Complying with the laws and regulations governing the industry and geographical region in which an organisation finds itself, should always be a priority for any organisation. Failure to adhere to laws and regulations affecting the organisation could result in the organisation being liable for large fines or penalties for breach of the relevant laws and regulations.

McQuire (2012) indicated that organisations operating in highly regulated industries cannot afford any compromise to customer data records or the compliance requirements governing these industries. McQuire stated in the same research paper, that in certain countries like Germany, the federal law concerning data protection stipulates that German company data must reside in Europe.

Research conducted by Vodafone (2012) indicated that it is important that organisations ensure regulatory compliance, especially where employees are permitted to run corporate email on their devices as this may be subject to some form of communication regulations. They also noted that it is more difficult to ensure compliance where the organisation does not own the device.

Where an employee uses software purchased for their personal mobile devices under "personal use" licenses for business purposes, the organisation may not be complying with the rules governing the use of the software and may be liable for the additional costs (O'Brien, 2013).

There is a possibility that it will be more challenging for organisations to ensure that they are complying with the rules and regulations affecting them in the future. This is especially true with the constant technological advancements taking place and the manner in which data is shared and transferred from one device to the next.

3.2.7 Obsolescence

New mobile devices are released into the market on a regular basis. The manufacturers of these devices have done a great job in convincing individuals to upgrade from their existing devices, even though the new device may not offer much more than the user is currently receiving from their existing device.

Entner (2011) indicated that of the 14 countries which he investigated to determine handset replacement lifecycles, South Africans took 38.2 months before buying a new mobile telephone. The research indicated that the

handset replacement lifecycles for South Africans in the previous year was 46.3 months.

The most common practice with mobile phone companies is to have a new model or an updated model every year. Stylistic obsolescence is one of the driving phenomenon that is occurring (particularly) in the mobile phone industry (Keeble, 2013; Maycroft 2009).

If employees continue to upgrade their devices on a regular basis, it will have a direct impact on the IT department. They may not be able to cope with the regular upgrades and they may not be able to identify the risks associated with all the new devices being deployed into the system.

3.3 Operational concerns and risks

Ability of IT to support BYOD programs

The tasks performed by employees in IT departments at organisations have changed substantially over the past decade. In the past these employees were mainly responsible for configuring, installing, maintaining and operating the hardware and software used by employees at the organisation's offices. Many organisations deployed corporate owned palmtop-computers and Blackberry devices to key individuals within the organisation during the early to mid two thousands. The configurations of these devices were generally straight forward. The devices were used primarily to send emails and to retrieve key documents and presentations. With the deployment of these devices it meant that the employees in the IT department needed to gain an understanding on how these devices functioned. In the past two to three years, with increased popularity of individuals wanting to use their own mobile devices to access sensitive information relating to the organisation, the role of IT employee's has expanded yet again.

The security of mobile devices has become a top concern for many IT executives (IBM, 2011). The concern is further increased as the number of mobile devices coming in the next few years will outstrip IT's ability to keep the enterprise secure (Klossner, 2012). Kaspersky (2012) and Staut (2012) indicated that the average employee uses more than one mobile device to access the corporate network. BYOD therefore brings IT and security departments the challenge of having to implement and manage mobile security across an almost limitless range of devices and operating systems

Rose (2012) stated that IT departments now have the responsibility of managing and securing a wide range of mobile devices wanting to access their organisations' corporate data. Rose also indicated in the same article that research conducted by Forrester indicates that employees choose their own smartphones 70% of the time, with 48% of the devices picked without regard for IT support. Anderson (2012) stated that devices are evolving so rapidly that it is impractical to pre-approve each and every device brand and form-factor. Anderson also indicated that it was somewhat impractical to expect IT organizations to have the same level of support for each and every device that employees may bring to the workplace. (Anderson, 2012)

Employees' mobile devices which have not been configured and locked down by the company IT department, creates the opportunity for infiltration of malware, gaps in the firewall, and exfiltration of sensitive data. (Mansfield-Devine, 2012). The risk is further increased as some corporations intentionally have open ports, so that their employees can work in virtual environments. This is an opportunity for anyone on the Internet, who wishes to access a corporation's information system in an unauthorised manner (Markelj and Bernik, 2012).

BYOD has changed the manner in which IT departments now function. They are now required to have detailed knowledge of various mobile devices which employees could use to access the organisations network.

3.4 Summary of the incremental information technology strategic and operational risks and concerns identified.

Table 1 lists the risks and concerns which have been identified during the extensive literature review as well as the source used to identify the risks.

Table 1

Number	Summarised risk/concern	Description of risk / concern	Source
1) Malware			
	1.1 Deployment of malware into organisations system.	1.1 There is a risk that employees may purposefully or negligently deploy malware into the organisations computer system which may result in unauthorised access to sensitive information.	1.1 Ponemon Institute LLC, 2012.
	1.2 Malicious software targets smartphones and tablets.	1.2 There is a risk that new malicious software will target smartphones and tablets.	1.2 Drew, 2012; Kaspersky, 2012; Ponemon Institute LLC, 2012; IBM 2011.
	1.3 Hackers ability to control computer systems.	1.3 There is a risk that hackers will use malware to steal passwords of mobile device users and take control of the organisations computer systems (including smartphones and tablets).	1.3 Staut, 2012.
	1.4 Data stolen or damaged.	1.4 There is a risk that data on the user's mobile device may be stolen or damaged by malicious malware.	1.4 CISCO, 2013.

Number	Summarised risk/concern	Description of risk / concern	Source
1) Malware			
	1.5 Device disabled.	1.5 There is a risk that malware may disable the users mobile device resulting in the inability to perform tasks.	1.5 CISCO, 2013.
	1.6 Use of unapproved applications.	1.5 There is a risk that users of mobile devices may be using unapproved applications on their devices which may expose the organisation to malware attacks .	1.6 DAT, 2012.
2) Data Leakage			
	2.1 Data leakage is a great problem.	2.1 There is a risk that data leakage problems may occur at the organisation.	2.1 Willis, 2013b.
	2.2 Employees sync mobile device with infected home computer.	2.2 There is a risk that employees will sync their mobile devices which they use to access the organisations network to their home computers, which may be infected with malware.	2.2 Kaspersky, 2012.
	2.3 Unpatched vulnerabilities on home computer grants cybercriminals access to sensitive data.	2.3 There is a risk that unpatched vulnerabilities on the employees home computer will grant cybercriminals the ability to gain access to the sensitive mobile data that has been backed up, stored or synced onto the employee's home computer.	2.3 Kaspersky, 2012.

Number	Summarised risk/concern	Description of risk / concern	Source
2) Data Leakage			
	2.4 Loss of control over data stored in the Cloud.	2.4 There is a risk that data shared and stored via a Cloud may result in the organisation having a shadow infrastructure where they have little to no control of the data.	2.4 Anderson, 2013; IBM, 2011.
	2.5 Unauthorised access to sensitive data.	2.5 There is a risk that data stored in the cloud may be accessed by unauthorised individuals.	2.5 Anderson, 2013; IBM, 2011.
	2.6 Potential financial loss as a result of data breach.	2.6 There is a risk that a data breach could be financially costly for the organisation.	2.6 IBM, 2012.
3) Loss and theft			
	3.1Lost mobile devices create a security threat.	3.1 There is a risk that mobile devices which have been lost may contain confidential corporate information on it and this will create a serious security threat to the organisation.	3.1 Kaspersky, 2012.
	3.2 Criminals may gain access to confidential information.	3.2 There is a risk that criminals may access confidential information relating to the organisation from a stolen smartphone or tablet.	3.2 Staut, 2012.
	3.3 Information may not be password protected.	3.3 There is a risk that information on an employee's smartphone or tablet which has been lost or stolen may not be password protected and may result in unauthorised access to confidential information.	3.3 Staut, 2012; Ponemon Institute LLC, 2012.
	.		

Number	Summarised risk/concern	Description of risk / concern	Source
3) Loss or theft			
	3.4 Data may not be encrypted.	3.4 There is a risk that the confidential corporate related data transmitted to and from the employees mobile device may not be encrypted and may therefore be accessed by unauthorised individuals.	3.4. Staut, 2012.
	3.5 Mobile devices are easily stolen as a result of size.	3.5 There is a risk that mobile devices may be easily stolen as a result of these devices generally being small in size.	3.5 Markelj and Bernik,2012.
	3.6 Data on mobile device which has been lost or stolen may be compromised.	3.6 There is a risk that all of the data stored on a mobile device which has been lost or stolen may be accessed by unauthorised individuals if access to the mobile device or the data is not effectively controlled.	3.6 Evangelista, 2013.
	3.7 Lost or stolen mobile devices may have personally identifying and confidential client information on it.	3.7 There is a risk that a lost or stolen mobile device may contain personally identifying or confidential client information on the device.	3.7 Drew, 2012.
	3.8 Organisation cannot remotely wipe lost mobile device.	3.8 There is a risk that the organisation does not have the ability to remotely wipe a device if a smartphone is lost or stolen.	3.8 Rose, 2012.
	3.9 Employees don't know what to do when device is lost or stolen.	3.9 There is a risk that as a result of employees not knowing what to do if their device was lost or stolen that unauthorised individuals may gain access to sensitive corporate information.	3.9 Rose, 2012.

Number	Summarised risk/concern	Description of risk / concern	Source
4) Connection			
	4.1 Bluetooth device may be discoverable.	4.1 There is a risk that the Bluetooth on the mobile device on which sensitive corporate data is stored is set on discoverable mode which may grant access unauthorised individuals access to the data.	4.1 Cisco, 2013.
	4.2 Unauthorised data downloads	4.2 There is a risk that an unauthorised individual may connect to the mobile device and download the private data located on the mobile device.	4.2 Cisco, 2013
	4.3 Non-authenticated devices connecting to network.	4.3 There is a risk that non-authenticated devices may gain access to the organisations network by connecting through an authenticated device.	4.3 Anderson, 2013.
	4.4 Bluetooth and Wi-Fi technology are easily infected.	4.4 There is a risk that Bluetooth and Wi-Fi technology can be easily infected with malware which may result in the organisations network also being infected.	4.4 IBM, 2011.
	4.5 Data transmitted may be compromised.	4.5 There is a risk that the data transmitted via Bluetooth or Wi-Fi technology is compromised.	4.5 IBM, 2011.

Number	Summarised risk/concern	Description of risk / concern	Source
5) Web based applications			
	5.1 Applications downloaded may steal or damage data.	5.1 There is a risk that applications downloaded may contain malware which may steal or damage company data stored on the mobile device.	5.1 IBM, 2011; IBM, 2012.
	5.2 Unapproved applications may be stored on mobile devices.	5.2 There is a risk that unapproved applications on employee mobile devices may contain malware.	5.2 DAT, 2012.
	5.3 Unapproved applications may not be easily detectable.	5.3 There is a risk that the unapproved applications may not be easily detectable and may result in malware entering the organisations system undetected.	5.3 DAT, 2012.
	5.4 Employees unaware of risky applications.	5.4 There is a risk that employees are unaware of which popular applications are security risks and may result in the employee downloading a malicious application which may infect the organisations system.	5.4 Rose, 2012.
6) Compliance			
	6.1Organisation may not be complying with laws and regulations.	6.1 There is a risk that corporate data stored on the employees mobile device may be compromised which could result in the organisation not complying with the laws and regulations affecting the industry in which the organisation operates.	6.1 McQuire (2012).

Number	Summarised risk/concern	Description of risk / concern	Source
6) Compliance			
	6.2 Organisation may be unaware of specific geographical laws and regulations.	6.2 Certain geographical regions have unique laws and regulations such as the data protection laws in Europe which states that data must reside in Europe. The risk is that an employee may download sensitive corporate data onto their mobile device and leave Europe with the sensitive data on the device resulting in the organisation not complying with the relevant laws and regulations.	6.2 McQuire (2012).
	6.3 Communication laws may be violated.	6.3 There is a risk that organisations may not comply with communication laws. This would arise where employees are not permitted to transfer corporate data to their personal devices.	6.3 Vodafone, 2012.
	6.4 Organisations may not be able to ensure compliance on employee owned devices.	6.4 There is a risk that the organisation may not be able to ensure regulatory compliance in instances where the organisation does not own the mobile device.	6.4 Vodafone, 2012.
	6.5 Personal use software may be used for business purposes.	6.5 There is a risk that an employee may be using software on a mobile device designated under a personal use license for business purposes resulting in the organisation contravening the terms of use of the software.	6.5 O'Brien, 2013.
	6.6 Potential additional costs to be incurred by organisation.	6.6 There is a risk that the organisation may be liable for the additional costs where employees have breached software license agreements.	6.6 O'Brien, 2013.

Number	Summarised risk/concern	Description of risk / concern	Source
7) IT Support			
	7.1 IT may not be able to manage all mobile devices.	7.1There is a risk that IT may not be able to manage the wide range of mobile devices which the employees of the organisation use to access sensitive corporate data.	7.1 Rose, 2012.
	7.2 IT may not be able to secure all mobile devices.	7.2 There is a risk that IT may not be able to secure all of the mobile devices which the employees of the organisation use to access sensitive corporate data.	7.2 Klossner, 2012; Rose, 2012.
	7.3 IT may not be able to successfully implement mobile security.	7.3 There is a risk that IT and security departments may not be able to successfully implement mobile security as a result of the almost limitless range of devices and operating systems being used in the organisation.	7.3 Kaspersky, 2012; Staut 2012.
	7.4 Employees may select a device without considering IT support.	7.4 Employees at the organisation may choose a mobile device without regard for IT support. The risk is that the IT department may not be able to assist employees when their devices are down and this will affect the employees' productivity and ability to complete their work related tasks.	7.4 Rose, 2012.
	7.5 Employee mobile devices may not be configured or locked down.	7.5 There is a risk that employee mobile devices that are not configured and locked down by the IT department will result in an infiltration of malware and an exfiltration of sensitive corporate data.	7.5 Mansfield-Devine, 2012.

Number	Summarised risk/concern	Description of risk / concern	Source
7) IT Support			
	7.6 IT may not pre-approve all mobile devices.	7.6 There is a risk that employees may use devices to access sensitive corporate data which has been determined by the IT department as devices which expose the organisation to security risks.	7.6 Anderson, 2013.
	7.7 IT may not be able to provide same level of support to all mobile devices.	7.7 There is a risk that IT may not be able to provide the same level of support for each and every device that employees bring to the workplace. This may result in the employee not being able to perform their work related tasks in an effective and efficient manner.	7.7 Anderson, 2013.
	7.8 The organisation may leave certain network ports open for ease of connection for employee owned devices. .	7.8 There is a risk that the organisation has open ports for employee owned mobile devices. This may create an opportunity for anyone on the Internet to access a corporation's information system unauthorised. .	7.8 Markelj and Bernik, 2012.

Number	Summarised risk/concern	Description of risk / concern	Source
8) Obsolescence			
	8.1 Mobile device life cycle may shorten.	8.1 The mobile device life cycle may shorten. The risk is that the organisation may not be able to keep abreast with the all the new devices being used by their employees and this may result in the risks associated with these devices not being adequately and timeously addressed.	8.1Entner, 2011.
	8.2 Mobile devices may have planned obsolescence built into them.	8.2 Manufacturers of mobile devices have planned obsolescence built into their devices. The risk is that the organisation may not be able to keep abreast with the all the new devices being used by their employees and this may result in the risks associated with these devices not being adequately and timeously addressed.	8.2 Keeble, 2013; Maycroft 2009.

The risks identified in the table 1 need to be reduced to an acceptable level. This is best done by making use of an appropriate control framework to identify key controls which can be deployed to reduce the risks to an acceptable level.

4. CHAPTER 4: SELECTION OF FRAMEWORK

4.1 Selection of control framework

A control framework is a data structure that organises and categorises an organisation's internal controls, which are practices and procedures established to create business value and minimize risk (Rouse, 2011).

The Institute of directors of Southern Africa (2009) stated that IT governance can be considered as a framework that supports effective and efficient management of IT resources to facilitate the achievement of a company's strategic objectives.

Some notable information technology frameworks include Prince 2, ITIL and COBIT 5.

4.2 COBIT 5

COBIT 5 is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks (ISACA, 2012c).

COBIT 5 provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT (ISACA, 2012c).

Stroud (2012) stated in a webinar conducted by ISACA, that COBIT 5 helps enterprises create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use. The framework addresses both business and IT functional areas across an enterprise and considers the IT related interests of internal and external stakeholders.

COBIT 5 is based on five key principles (ISACA, 2012c).

The five key principles being:

1. Principle 1: Meeting Stakeholder Needs
2. Principle 2: Covering the Enterprise End-to-End
3. Principle 3: Applying a Single, Integrated Framework
4. Principle 4: Enabling a Holistic Approach
5. Principle 5: Separating Governance From Management

COBIT 5 process reference model divides the governance and management processes of enterprise IT into two main process domains, namely: governance and management (ISACA, 2012c).

The governance domain contains five governance processes; namely:

- Ensure Governance Framework Setting and Maintenance,
- Ensure Benefits delivery,
- Ensure Risk Optimisation,
- Ensure Resource Optimisation, and
- Ensure Stakeholder Transparency.

Within each process mentioned above, evaluate, direct and monitor (EDM) practices are defined (ISACA, 2012c).

- Evaluate, Direct and Monitor (EDM): which provides the organisation with guidance on how they should govern and manage their IT enabled business investments.

The management domain contains four domains, in line with the responsibility areas of plan, build, run and monitor (PBRM), and provides an end-to-end coverage of IT (ISACA, 2012c).

The four domains

- Align, Plan and Organise (APO): which provides guidance for planning and organising acquisitions which are to made by the organisation.

- Build, Acquire and Implement (BAI): which provides guidance on the processes required to acquire and implement IT solutions.

- Deliver, Service and Support (DSS): which provides guidance for servicing and supporting IT solutions.

- Monitor, Evaluate and Assess (MEA): which provides directors with guidance on how they can monitor and evaluate the acquisition process and the internal controls which have been implemented. This will help ensure that acquisitions are properly managed and executed.

In order for an organisation to reduce identified risks to an acceptable level, they need to implement internal controls.

For the purpose of this study it was determined that the controls identified must be in line with principles of internal control as stated in the COSO 2013 framework.

The committee of sponsoring organisations of the Treadway Commission (Treadway Commission, 2013) stated that internal control helps entities achieve important objectives and sustain and improve performance.

For management to conclude that its system of internal control is effective, all five components (control environment, risk assessment, control activities, information and communication, and monitoring activities) of internal control and all relevant principles must be present and functioning (McNally, 2013).

The five components can be further broken down into 17 principles, namely:

- Control environment
  - Demonstrates commitment to integrity and ethical values,
  - Exercises oversight responsibility,
  - Establishes structure, authority, and responsibility,
  - Demonstrates commitment to competence, and
  - Enforces accountability.

- Risk assessment
  - Specifies suitable objectives,
  - Identifies and analyzes risk,
  - Assesses fraud risk, and
  - Identifies and analyzes significant change.

- Control activities
  - Selects and develops control activities,
  - Selects and develops general controls over technology, and
  - Deploys through policies and procedures.

- Information and communication
  - Uses relevant information,
  - Communicates internally, and
  - Communicates externally.

- Monitoring activities
  - Conducts ongoing and/or separate evaluations, and
  - Evaluates and communicates deficiencies.

The COSO board believe that each principle adds value to the organisation and is suitable for all organisations (McNally, 2013).

The COBIT 5 framework was released in 2012. Significant improvements were made to the previous version (COBIT 4.1) (IT Governance Institute (ITGI), 2007). As every enterprise has different objectives, an enterprise can customise COBIT 5 to suit its own context through the goals cascade, translating high-level enterprise goals into manageable, specific, IT-related goals and mapping these to specific processes and practices (ISACA, 2012c).

The framework, if used correctly, will enable the organisation to identify internal controls in line with the principles of internal control as stated in the COSO 2013 framework. It was therefore determined that COBIT 5 was an appropriate framework against which the incremental information technology strategic and operational risks arising from the deployment of a BYOD program could be mapped.

4.3 Identification of applicable COBIT 5 processes which affect BYOD Programs

As noted in 4.2 organisations can customise COBIT 5 to suit their own context. In order to identify which processes are applicable to an organisation which has deployed a BYOD program, Table 2 was created. Table 2 further illustrates which of the 37 COBIT 5 processes are applicable for the purposes of this study. This was determined by conducting the extensive literature review in chapter 3.

Table 2

COBIT 5 Process			**Relevant to BYOD**	**Applicable to research**
Governance domain				
Evaluate, Direct and Monitor	EDM01	Ensure Governance Framework Setting and Maintenance	Yes	Yes
	EDM02	Ensure Benefits Delivery	No	No
	EDM03	Ensure Risk Optimisation	Yes	Yes
	EDM04	Ensure Resource Optimisation	Yes	Yes
	EDM05	Ensure Stakeholder Transparency	No	No
Management domain				
Align, Plan and Organise	APO01	Manage the IT Management Framework	Yes	Yes
	APO02	Manage Strategy	Yes	No
	APO03	Manage Enterprise Architecture	Yes	No
	APO04	Manage Innovation	Yes	Yes
	APO05	Manage Portfolio	No	No
	APO06	Manage Budget and Costs	Yes	Yes
	APO07	Manage Human Resources	No	No

COBIT 5 Process			Relevant to BYOD	Applicable to research
	Management domain			
Align, Plan and Organise	APO08	Manage Relationships	Yes	No
	APO09	Manage Service Agreements	Yes	No
	APO10	Manage Suppliers	No	No
	APO11	Manage Quality	Yes	No
	APO12	Manage Risk	Yes	Yes
	APO13	Manage Security	Yes	Yes
Build, Acquire and Implement	BAI01	Manage Programmes and Projects	Yes	No
	BAI02	Manage Requirements Definition	Yes	No
	BAI03	Manage Solutions Identification and Build	Yes	No
	BAI04	Manage Availability and Capacity	Yes	No
	BAI05	Manage Organisational Change Enablement	Yes	No
	BAI06	Manage Changes	Yes	No
	BAI07	Manage Change Acceptance and Transitioning	Yes	No
	BAI08	Manage Knowledge	Yes	No
	BAI09	Manage Assets	Yes	Yes
	BAI10	Manage Configuration	Yes	No

COBIT 5 Process			Relevant to BYOD	Applicable to research
	Management domain			
Deliver, Service and Support	DSS01	Manage Operations	Yes	Yes
	DSS02	Manage Service Requests and Incidents	Yes	Yes
	DSS03	Manage Problems	Yes	Yes
	DSS04	Manage Continuity	Yes	No
	DSS05	Manage Security Services	Yes	Yes
	DSS06	Manage Business Process Controls	Yes	Yes
Monitor, Evaluate and Assess	MEA01	Monitor, Evaluate and Assess Performance and Conformance	Yes	No
	MEA02	Monitor, Evaluate and Assess the System of Internal Control	Yes	No
	MEA03	Monitor, Evaluate and Assess Compliance With External Requirements	Yes	Yes

As noted in Table 2 of this research, not all of the processes are considered applicable to an organisation which has deployed a BYOD program.

Table 3 gives a detailed listing of what each processes means. The definitions of the processes were obtained from COBIT 5 Enabler processing guide (ISACA, 2012a). A brief explanation as to why a process was considered applicable or in certain instances why a certain process was not applicable for the purpose of this research has been included in this table.

Table 3

COBIT 5 Process			**Description**
Evaluate, Direct and Monitor	EDM01	Ensure Governance Framework Setting and Maintenance	Analyse and articulate the requirements for the governance of enterprise IT, and put in place and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives (ISACA, 2012a).
	Applicable to the research	**Yes**	**Explanation:** It is important that the organisation adopts a BYOD program if it assists the organisation in achieving its business imperatives. Once it has been determined that BYOD will add value to the organisation, it is important that proper structures, processes and practices are put in place in order to ensure that the business imperatives are met and that any risks associated with deploying a BYOD program are reduced to an acceptable level.
	EDM02	Ensure Benefits Delivery	Optimise the value contribution to the business from the business processes, IT services and IT assets resulting from investments made by IT at acceptable costs (ISACA, 2012a).
	Applicable to the research	**No**	**Explanation:** The employee is primarily responsible for investment in the mobile device which is used to access personal and corporate information.

COBIT 5 Process			Description
Evaluate, Direct and Monitor	EDM03	Ensure Risk Optimisation	Ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and that risk to enterprise value related to the use of IT is identified and managed (ISACA, 2012a).
	Applicable to the research	**Yes**	**Explanation:** Prior to deciding to launch a BYOD program, it is important that those charged with governance at the organisation first identify the entity specific risks that they will be exposed to as a result of adopting a BYOD program and they should determine to what extent they would like to be protected from these risks as this will assist them in determining what controls they should be implementing.
	EDM04	Ensure Resource Optimisation	Ensure that adequate and sufficient IT-related capabilities (people, processes and technology) are available to support enterprise objectives effectively at optimal cost (ISACA, 2012a).
	Applicable to the research	**Yes**	**Explanation:** In order to successfully run a BYOD program, the organisation needs to make sure the IT department has the necessary knowledge, skills and time available to properly manage and support the BYOD program.
	EDM05	Ensure Stakeholder Transparency	Ensure that enterprise IT performance and conformance measurement and reporting are transparent, with stakeholders approving the goals and metrics and the necessary remedial actions (ISACA, 2012a).
	Applicable to the research	**No**	**Explanation:** It is not necessary to report to the outside stakeholders on the successful adoption or running of the BYOD program.

COBIT 5 Process			Description
Align, Plan and Organise	APO01	Manage the IT Management Framework	Clarify and maintain the governance of enterprise IT mission and vision. Implement and maintain mechanisms and authorities to manage information and the use of IT in the enterprise in support of governance objectives in line with guiding principles and policies (ISACA, 2012a).
	Applicable to the research	**Yes**	**Explanation:** The adoption of a BYOD program and the running thereof should be to support the overall governance objectives of the organisation.
	APO02	Manage Strategy	Provide a holistic view of the current business and IT environment, the future direction, and the initiatives required to migrate to the desired future environment. Leverage enterprise architecture building blocks and components, including externally provided services and related capabilities to enable nimble, reliable and efficient response to strategic objectives (ISACA, 2012a).
	Applicable to the research	**No**	**Explanation:** The BYOD program would be a current initiative which the organisation has adopted. Whilst it may be a current business strategy of the organisation, it was not included as part of the focus of this research.
	APO03	Manage Enterprise Architecture	Establish a common architecture consisting of business processes, information, data, application and technology architecture layers for effectively and efficiently realising enterprise and IT strategies by creating key models and practices that describe the baseline and target architectures. Define requirements for taxonomy, standards, guidelines, procedures, templates and tools, and provide a linkage for these components. Improve alignment, increase agility, improve quality of information and generate potential cost savings through initiatives such as re-use of building block components (ISACA, 2012a).
	Applicable to the research	**No**	**Explanation:** Whilst having proper architectures in place to govern the BYOD program adopted by an organisation is important, it was not included as part of the focus of this research.

COBIT 5 Process			Description
Align, Plan and Organise	APO04	Manage Innovation	Maintain an awareness of information technology and related service trends, identify innovation opportunities, and plan how to benefit from innovation in relation to business needs. Analyse what opportunities for business innovation or improvement can be created by emerging technologies, services or IT-enabled business innovation, as well as through existing established technologies and by business and IT process innovation. Influence strategic planning and enterprise architecture decisions (ISACA, 2012a).
	Applicable to the research	**No**	**Explanation:** BYOD is an innovative business trend. There are lots of benefits which the organisation can obtain through the successful implementation of a BYOD program. Whilst this was not the core focus of this research, a few benefits have been identified in 3.1.
	APO05	Manage Portfolio	Execute the strategic direction set for investments in line with the enterprise architecture vision and the desired characteristics of the investment and related services portfolios, and consider the different categories of investments and the resources and funding constraints. Evaluate, prioritise and balance programmes and services, managing demand within resource and funding constraints, based on their alignment with strategic objectives, enterprise worth and risk. Move selected programmes into the active services portfolio for execution. Monitor the performance of the overall portfolio of services and programmes, proposing adjustments as necessary in response to programme and service performance or changing enterprise priorities (ISACA, 2012a).
	Applicable to the research	**No**	**Explanation:** Whilst BYOD may form part of the overall investment or related portfolios of the organisation, it was assumed that the BYOD program was a priority for the purpose of this research and hence no adjustments needed to be made.

COBIT 5 Process			Description
Align, Plan and Organise	APO06	Manage Budget and Costs	Manage the IT-related financial activities in both the business and IT functions, covering budget, cost and benefit management, and prioritisation of spending through the use of formal budgeting practices and a fair and equitable system of allocating costs to the enterprise. Consult stakeholders to identify and control the total costs and benefits within the context of the IT strategic and tactical plans, and initiate corrective action where needed (ISACA, 2012a).
	Applicable to the research	**No**	**Explanation:** The organisation needs to identify that there is a financial benefit which they can derive before adopting a BYOD program. Whilst this is important, it was not included as part of the focus of this research.
	APO07	Manage Human Resources	Provide a structured approach to ensure optimal structuring, placement, decision rights and skills of human resources. This includes communicating the defined roles and responsibilities, learning and growth plans, and performance expectations, supported with competent and motivated people (ISACA, 2012a).
	Applicable to the research	**No**	**Explanation:** BYOD should not directly impact the management of human resources at the organisation. Whilst the skill and ability of the IT department needs to be considered when adopting a BYOD program, it was not included as part of the focus of this research.
	APO08	Manage Relationships	Manage the relationship between the business and IT in a formalised and transparent way that ensures a focus on achieving a common and shared goal of successful enterprise outcomes in support of strategic goals and within the constraint of budgets and risk tolerance. Base the relationship on mutual trust, using open and understandable terms and common language and a willingness to take ownership and accountability for key decisions (ISACA, 2012a).
	Applicable to the research	**No**	**Explanation:** Whilst the relationship between those employed in the operational side of the organisation and the IT side of the organisation is important, the quality of their relationship was not included as part of the focus of this research.

COBIT 5 Process			Description
Align, Plan and Organise	APO09	Manage Service Agreements	Align IT-enabled services and service levels with enterprise needs and expectations, including identification, specification, design, publishing, agreement, and monitoring of IT services, service levels and performance indicators (ISACA, 2012a).
	Applicable to the research	**No**	**Explanation:** It is important that the organisation first identify its business imperatives. If it was concluded that the adoption of the BYOD program would assist in the achieving of the organisations business imperatives then the BYOD program should be adopted. The considerations of whether or not a BYOD program would assist the organisation in achieving their business imperatives was not included as part of the focus of this research.
	APO10	Manage Suppliers	Manage IT-related services provided by all types of suppliers to meet enterprise requirements, including the selection of suppliers, management of relationships, management of contracts, and reviewing and monitoring of supplier performance for effectiveness and compliance (ISACA, 2012a).
	Applicable to the research	**No**	**Explanation:** The adoption of a BYOD program does not involve the supply of any goods or services by outside suppliers directly to the organisation. The employee deals with the supplier of the mobile device.
	APO11	Manage Quality	Define and communicate quality requirements in all processes, procedures and the related enterprise outcomes, including controls, ongoing monitoring, and the use of proven practices and standards in continuous improvement and efficiency efforts (ISACA, 2012a).
	Applicable to the research	**No**	**Explanation:** Defining the communication of quality requirements in all processes and procedures is of key importance for every organisation. The defining and communication of BYOD processes was however not included as part of the focus of this research.

COBIT 5 Process			Description
Align, Organise and Plan	APO12	Manage Risk	Continually identify, assess and reduce IT-related risk within levels of tolerance set by enterprise executive management (ISACA, 2012a).
	Applicable to the research	**Yes**	**Explanation:** It should be a priority for the organisation to continually identify, assess and reduce the risks that arise as a result of the adoption of a BYOD program. Failure to do so could have adverse consequences on the organisation.
	APO13	Manage Security	Define, operate and monitor a system for information security management (ISACA, 2012a).
	Applicable to the research	**Yes**	**Explanation:** Security of the corporate information should be a priority at all times. The safety of information is definitely a concern in a BYOD as a result of cyber theft.

COBIT 5 Process			Description
Build, Acquire and Implement	BAI01	Manage Programmes and Projects	Manage all programmes and projects from the investment portfolio in alignment with enterprise strategy and in a co-ordinated way. Initiate, plan, control, and execute programmes and projects, and close with a post-implementation review (ISACA, 2012a).
	Applicable to the research	**No**	**Explanation:** The BYOD program needs to be managed as one of the organisations programs. The management aspect of a BYOD program was however not included as part of the focus of this research.
	BAI02	Manage Requirements Definition	Identify solutions and analyse requirements before acquisition or creation to ensure that they are in line with enterprise strategic requirements covering business processes, applications, information/data, infrastructure and services. Co-ordinate with affected stakeholders the review of feasible options including relative costs and benefits, risk analysis, and approval of requirements and proposed solutions (ISACA, 2012a).
	Applicable to the research	**No**	**Explanation:** It is essential that the organisation first conduct a detailed analysis as to whether or not a BYOD program will assist them in the achievement of their business imperatives. The pre-adoption analysis of a BYOD program and the feasibility thereof was however not considered as part of this research.
	BAI03	Manage Solutions Identification and Build	Establish and maintain identified solutions in line with enterprise requirements covering design, development, procurement/sourcing and partnering with suppliers/vendors. Manage configuration, test preparation, testing, requirements management and maintenance of business processes, applications, information/data, infrastructure and services (ISACA, 2012a).
	Applicable to the research	**No**	**Explanation:** The deployment of a BYOD program may be one of the solutions which an organisation could employ in order to achieve its business imperatives. This was however not considered as part of this research.

COBIT 5 Process			Description
Build, Acquire and Implement	BAI04	Manage Availability and Capacity	Balance current and future needs for availability, performance and capacity with cost-effective service provision. Include assessment of current capabilities, forecasting of future needs based on business requirements, analysis of business impacts, and assessment of risk to plan and implement actions to meet the identified requirements (ISACA, 2012a).
	Applicable to the research	**No**	**Explanation:** The availability of enough skilled IT staff to support a BYOD program may be something that an organisation should be interested in. It was however not considered as part of this research.
	BAI05	Manage Organisational Change Enablement	Maximise the likelihood of successfully implementing sustainable enterprisewide organisational change quickly and with reduced risk, covering the complete life cycle of the change and all affected stakeholders in the business and IT (ISACA, 2012a).
	Applicable to the research	**No**	**Explanation:** The adoption of a BYOD program for the very first time by an organisation will definitely affect all the stakeholders in the organisation. The first time adoption of a BYOD program at an organisation was however not considered as part of this research.
	BAI06	Manage Changes	Manage all changes in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure. This includes change standards and procedures, impact assessment, prioritisation and authorisation, emergency changes, tracking, reporting, closure and documentation (ISACA, 2012a).
	Applicable to the research	**No**	**Explanation:** The initial adoption of a BYOD program by an organisation will definitely require significant attention. It would be a change from the normal way of accessing and processing sensitive corporate information. The initial adoption of a BYOD program at an organisation was however not considered as part of this research.

COBIT 5 Process			Description
Build, Acquire and Implement	BAI07	Manage Change Acceptance and Transitioning	Formally accept and make operational new solutions, including implementation planning, system and data conversion, acceptance testing, communication, release preparation, promotion to production of new or changed business processes and IT services, early production support, and a post-implementation review (ISACA, 2012a).
	Applicable to the research	**No**	**Explanation:** The initial period from pre adoption to initial adoption of the BYOD program needs to be planned successfully to ensure that all significant risks have been identified and that sensitive corporate data is safeguarded at all times. The initial adoption of a BYOD program at an organisation was however not considered as part of this research.
	BAI08	Manage Knowledge	Maintain the availability of relevant, current, validated and reliable knowledge to support all process activities and to facilitate decision making. Plan for the identification, gathering, organising, maintaining, use and retirement of knowledge (ISACA, 2012a).
	Applicable to the research	**No**	**Explanation:** It is important that the IT department have the relevant skills in order to manage and support a BYOD program. The maintenance of knowledge to be able to do so successfully was however not considered as part of this research.
	BAI09	Manage Assets	Manage IT assets through their life cycle to make sure that their use delivers value at optimal cost, they remain operational (fit for purpose), they are accounted for and physically protected, and those assets that are critical to support service capability are reliable and available. Manage software licenses to ensure that the optimal number are acquired, retained and deployed in relation to required business usage, and the software installed is in compliance with license agreements (ISACA, 2012a).

COBIT 5 Process			Description
Build, Acquire and Implement	**Applicable to the research**	**Yes**	**Explanation:** The organisation does not own the mobile devices being used to access the organisations sensitive information. The IT department however should be in a position where they are able to assist the users the mobile devices with certain technical issues that arise with the devices. It is also extremely important that software licenses of these devices are understood as the organisation may be in breach if the employee uses software on the mobile device for business purposes when in fact it's a personal use software license which the employee possess.
	BAI10	Manage Configuration	Define and maintain descriptions and relationships between key resources and capabilities required to deliver IT-enabled services, including collecting configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository (ISACA, 2012a).
	Applicable to the research	**No**	**Explanation:** It is extremely important that the configurations of all devices connecting to the organisations network be defined and maintained. This is applicable in a BYOD environment as devices will be connecting to the organisations network. Defining and maintaining descriptions and relationships of resources and capabilities required by IT-enabled services was however not considered as part of this research.

COBIT 5 Process			Description
Deliver, Service and Support	DSS01	Manage Operations	Co-ordinate and execute the activities and operational procedures required to deliver internal and outsourced IT services, including the execution of pre-defined standard operating procedures and the required monitoring activities (ISACA, 2012a).
	Applicable to the research	**Yes**	**Explanation:** The execution of IT procedures effectively in managing and securing mobile devices is essential to ensure the safeguarding of sensitive corporate information.
	DSS02	Manage Service Requests and Incidents	Provide timely and effective response to user requests and resolution of all types of incidents. Restore normal service; record and fulfil user requests; and record, investigate, diagnose, escalate and resolve incidents (ISACA, 2012a).
	Applicable to the research	**Yes**	**Explanation:** The IT department should be in a position to assist the mobile device user with support and with troubleshooting required by the user which will enable them the ability to access and process work related activities on their mobile devices.
	DSS03	Manage Problems	Identify and classify problems and their root causes and provide timely resolution to prevent recurring incidents. Provide recommendations for improvements (ISACA, 2012a).
	Applicable to the research	**Yes**	**Explanation:** The IT department should be in a position to assist the mobile device user with support with troubleshooting required by the user to enable them the ability to access and process work related activities on their mobile devices.
	DSS04	Manage Continuity	Establish and maintain a plan to enable the business and IT to respond to incidents and disruptions in order to continue operation of critical business processes and required IT services and maintain availability of information at a level acceptable to the enterprise (ISACA, 2012a).

COBIT 5 Process			Description
Deliver, Service and Support	**Applicable to the research**	**No**	**Explanation:** It is important that the organisation have a plan in place for incidents such as mobile device or Wi-Fi down time as this will disrupt the organisations ability to function properly. The establishment and maintenance of a plan of this nature was however not considered as part of the research conducted.
	DSS05	Manage Security Services	Protect enterprise information to maintain the level of information security risk acceptable to the enterprise in accordance with the security policy. Establish and maintain information security roles and access privileges and perform security monitoring (ISACA, 2012a).
	Applicable to the research	**Yes**	**Explanation:** It is essential that the organisation conduct a proper risk analysis (which will include security related risks) in relation to the adoption of a BYOD program.
	DSS06	Manage Business Process Controls	Define and maintain appropriate business process controls to ensure that information related to and processed by in-house or outsourced business processes satisfies all relevant information control requirements. Identify the relevant information control requirements and manage and operate adequate controls to ensure that information and information processing satisfy these requirements (ISACA, 2012a).
	Applicable to the research	**Yes**	**Explanation:** Once the risk analysis has been conducted, it is important that the organisation identify suitable controls which will reduce the risks to an acceptable level.

COBIT 5 Process			Description
Monitor, Evaluate and Assess	MEA01	Monitor, Evaluate and Assess Performance and Conformance	Collect, validate and evaluate business, IT and process goals and metrics. Monitor that processes are performing against agreed-on performance and conformance goals and metrics and provide reporting that is systematic and timely (ISACA, 2012a).
	Applicable to the research	**No**	**Explanation:** It is essential that the success of the BYOD program be monitored by the organisation. Failure to do so could result in the organisation suffering major losses (e.g. data theft). The monitoring of the success of the BYOD program was however not considered as part of this research.
	MEA02	Monitor, Evaluate and Assess the System of Internal Control	Continuously monitor and evaluate the control environment, including self-assessments and independent assurance reviews. Enable management to identify control deficiencies and inefficiencies and to initiate improvement actions. Plan, organise and maintain standards for internal control assessment and assurance activities (ISACA, 2012a).
	Applicable to the research	**No**	**Explanation:** It is essential that the control environment and the controls affecting the BYOD program be monitored on a regular basis. Failure to do so could result in the organisation suffering major losses (e.g. data theft). The monitoring of the controls affecting the BYOD program was however not considered as part of this research.

COBIT 5 Process			Description
	MEA03	Monitor, Evaluate and Assess Compliance With External Requirements	Evaluate that IT processes and IT-supported business processes are compliant with laws, regulations and contractual requirements. Obtain assurance that the requirements have been identified and complied with, and integrate IT compliance with overall enterprise compliance (ISACA, 2012a).
	Applicable to the research	**Yes**	**Explanation:** It is essential that the organisation evaluate whether or not they are complying with the rules and regulations affecting the organisation. This is especially true in a BYOD environment where different industries and different geographical regions have different rules and regulations which govern them. The organisation should map the risks and controls indentified to reduce the risks to an acceptable level.

Table 4 maps the COBIT 5 processes which have been identified as being relevant for the purposes of this research to the risks identified in table 1.

Table 4

	Evaluate, Direct and Monitor			**Align, Plan and Organise**			**Build, Acquire and Implement**	**Deliver, Service and Support**					**Monitor, Evaluate and Assess**
Risk	EDM 01	EDM 03	EDM 04	APO 01	APO 12	APO 13	BAI 09	DSS0 1	DSS 02	DSS 03	DSS 05	DSS 06	MEA 03
	Ensure Governance Framework Setting and Maintenance	Ensure Risk Optimisation	Ensure Resource Optimisation	Manage the IT Management Framework	Manage Risk	Manage Security	Manage Assets	Manage Operations	Manage Service Requests and Incidents	Manage Problems	Manage Security Services	Manage Business Process Controls	Monitor, Evaluate and Assess Compliance With External Requirements
1.1	✓	✓		✓	✓	✓					✓		
1.2	✓	✓		✓	✓	✓					✓		
1.3	✓	✓		✓	✓	✓					✓		

	Evaluate, Direct and Monitor			**Align, Plan and Organise**			**Build, Acquire and Implement**	**Deliver, Service and Support**					**Monitor, Evaluate and Assess**
Risk	EDM 01	EDM 03	EDM 04	APO 01	APO 12	APO 13	BAI 09	DSS0 1	DSS 02	DSS 03	DSS 05	DSS 06	MEA 03
	Ensure Governance Framework Setting and Maintenance	Ensure Risk Optimisation	Ensure Resource Optimisation	Manage the IT Management Framework	Manage Risk	Manage Security	Manage Assets	Manage Operations	Manage Service Requests and Incidents	Manage Problems	Manage Security Services	Manage Business Process Controls	Monitor, Evaluate and Assess Compliance With External Requirements
1.4	✓	✓		✓	✓	✓					✓		
1.5	✓	✓		✓	✓	✓					✓		
1.6	✓	✓		✓	✓	✓					✓		

	Evaluate, Direct and Monitor			**Align, Plan and Organise**			**Build, Acquire and Implement**	**Deliver, Service and Support**					**Monitor, Evaluate and Assess**
Risk	EDM 01	EDM 03	EDM 04	APO 01	APO 12	APO 13	BAI 09	DSS0 1	DSS 02	DSS 03	DSS 05	DSS 06	MEA 03
	Ensure Governance Framework Setting and Maintenance	Ensure Risk Optimisation	Ensure Resource Optimisation	Manage the IT Management Framework	Manage Risk	Manage Security	Manage Assets	Manage Operations	Manage Service Requests and Incidents	Manage Problems	Manage Security Services	Manage Business Process Controls	Monitor, Evaluate and Assess Compliance With External Requirements
2.1	✓	✓		✓	✓	✓					✓		
2.2	✓	✓		✓	✓	✓					✓		
2.3	✓	✓		✓	✓	✓					✓		
2.4	✓	✓		✓	✓	✓					✓		
2.5	✓	✓		✓	✓	✓					✓		
2.6	✓	✓		✓	✓	✓					✓		

	Evaluate, Direct and Monitor			**Align, Plan and Organise**			**Build, Acquire and Implement**	**Deliver, Service and Support**					**Monitor, Evaluate and Assess**
Risk	EDM 01	EDM 03	EDM 04	APO 01	APO 12	APO 13	BAI 09	DSS0 1	DSS 02	DSS 03	DSS 05	DSS 06	MEA 03
	Ensure Governance Framework Setting and Maintenance	Ensure Risk Optimisation	Ensure Resource Optimisation	Manage the IT Management Framework	Manage Risk	Manage Security	Manage Assets	Manage Operations	Manage Service Requests and Incidents	Manage Problems	Manage Security Services	Manage Business Process Controls	Monitor, Evaluate and Assess Compliance With External Requirements
3.1	✓	✓		✓	✓	✓					✓		
3.2	✓	✓		✓	✓	✓					✓		
3.3	✓	✓		✓	✓	✓					✓		
3.4	✓	✓		✓	✓	✓					✓		
3.5	✓	✓		✓	✓	✓					✓		

	Evaluate, Direct and Monitor			**Align, Plan and Organise**			**Build, Acquire and Implement**	**Deliver, Service and Support**					**Monitor, Evaluate and Assess**
Risk	EDM 01	EDM 03	EDM 04	APO 01	APO 12	APO 13	BAI 09	DSS0 1	DSS 02	DSS 03	DSS 05	DSS 06	MEA 03
	Ensure Governance Framework Setting and Maintenance	Ensure Risk Optimisation	Ensure Resource Optimisation	Manage the IT Management Framework	Manage Risk	Manage Security	Manage Assets	Manage Operations	Manage Service Requests and Incidents	Manage Problems	Manage Security Services	Manage Business Process Controls	Monitor, Evaluate and Assess Compliance With External Requirements
3.6	✓	✓		✓	✓	✓					✓	✓	✓
3.7	✓	✓		✓	✓	✓					✓	✓	✓
3.8	✓	✓		✓	✓	✓					✓	✓	✓
3.9	✓	✓		✓	✓	✓					✓	✓	✓

	Evaluate, Direct and Monitor			**Align, Plan and Organise**			**Build, Acquire and Implement**	**Deliver, Service and Support**					**Monitor, Evaluate and Assess**
Risk	EDM 01	EDM 03	EDM 04	APO 01	APO 12	APO 13	BAI 09	DSS0 1	DSS 02	DSS 03	DSS 05	DSS 06	MEA 03
	Ensure Governance Framework Setting and Maintenance	Ensure Risk Optimisation	Ensure Resource Optimisation	Manage the IT Management Framework	Manage Risk	Manage Security	Manage Assets	Manage Operations	Manage Service Requests and Incidents	Manage Problems	Manage Security Services	Manage Business Process Controls	Monitor, Evaluate and Assess Compliance With External Requirements
4.1	✓	✓		✓	✓	✓					✓		
4.2	✓	✓		✓	✓	✓					✓		
4.3	✓	✓		✓	✓	✓					✓		
4.4	✓	✓		✓	✓	✓					✓		
4.5	✓	✓		✓	✓	✓					✓		

	Evaluate, Direct and Monitor			**Align, Plan and Organise**			**Build, Acquire and Implement**	**Deliver, Service and Support**					**Monitor, Evaluate and Assess**
Risk	EDM 01	EDM 03	EDM 04	APO 01	APO 12	APO 13	BAI 09	DSS0 1	DSS 02	DSS 03	DSS 05	DSS 06	MEA 03
	Ensure Governance Framework Setting and Maintenance	Ensure Risk Optimisation	Ensure Resource Optimisation	Manage the IT Management Framework	Manage Risk	Manage Security	Manage Assets	Manage Operations	Manage Service Requests and Incidents	Manage Problems	Manage Security Services	Manage Business Process Controls	Monitor, Evaluate and Assess Compliance With External Requirements
5.1	✓	✓		✓	✓	✓					✓		
5.2	✓	✓		✓	✓	✓					✓	✓	
5.3	✓	✓		✓	✓	✓					✓	✓	
5.4	✓	✓		✓	✓	✓					✓	✓	

	Evaluate, Direct and Monitor			**Align, Plan and Organise**			**Build, Acquire and Implement**	**Deliver, Service and Support**					**Monitor, Evaluate and Assess**
Risk	EDM 01	EDM 03	EDM 04	APO 01	APO 12	APO 13	BAI 09	DSS0 1	DSS 02	DSS 03	DSS 05	DSS 06	MEA 03
	Ensure Governance Framework Setting and Maintenance	Ensure Risk Optimisation	Ensure Resource Optimisation	Manage the IT Management Framework	Manage Risk	Manage Security	Manage Assets	Manage Operations	Manage Service Requests and Incidents	Manage Problems	Manage Security Services	Manage Business Process Controls	Monitor, Evaluate and Assess Compliance With External Requirements
6.1	✓	✓		✓	✓	✓					✓	✓	✓
6.2	✓	✓		✓	✓	✓					✓	✓	✓
6.3	✓	✓		✓	✓	✓					✓	✓	✓
6.4	✓	✓		✓	✓	✓					✓	✓	✓

	Evaluate, Direct and Monitor			**Align, Plan and Organise**			**Build, Acquire and Implement**	**Deliver, Service and Support**					**Monitor, Evaluate and Assess**
Risk	EDM 01	EDM 03	EDM 04	APO 01	APO 12	APO 13	BAI 09	DSS0 1	DSS 02	DSS 03	DSS 05	DSS 06	MEA 03
	Ensure Governance Framework Setting and Maintenance	Ensure Risk Optimisation	Ensure Resource Optimisation	Manage the IT Management Framework	Manage Risk	Manage Security	Manage Assets	Manage Operations	Manage Service Requests and Incidents	Manage Problems	Manage Security Services	Manage Business Process Controls	Monitor, Evaluate and Assess Compliance With External Requirements
6.5	✓	✓		✓	✓	✓					✓	✓	✓
6.6	✓	✓		✓	✓	✓					✓	✓	✓

	Evaluate, Direct and Monitor			**Align, Plan and Organise**			**Build, Acquire and Implement**	**Deliver, Service and Support**					**Monitor, Evaluate and Assess**
Risk	EDM 01	EDM 03	EDM 04	APO 01	APO 12	APO 13	BAI 09	DSS0 1	DSS 02	DSS 03	DSS 05	DSS 06	MEA 03
	Ensure Governance Framework Setting and Maintenance	Ensure Risk Optimisation	Ensure Resource Optimisation	Manage the IT Management Framework	Manage Risk	Manage Security	Manage Assets	Manage Operations	Manage Service Requests and Incidents	Manage Problems	Manage Security Services	Manage Business Process Controls	Monitor, Evaluate and Assess Compliance With External Requirements
7.1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
7.2	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓	
7.3	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓	
7.4	✓	✓	✓	✓	✓	✓		✓			✓	✓	

	Evaluate, Direct and Monitor			**Align, Plan and Organise**			**Build, Acquire and Implement**	**Deliver, Service and Support**					**Monitor, Evaluate and Assess**
Risk	EDM 01	EDM 03	EDM 04	APO 01	APO 12	APO 13	BAI 09	DSS0 1	DSS 02	DSS 03	DSS 05	DSS 06	MEA 03
	Ensure Governance Framework Setting and Maintenance	Ensure Risk Optimisation	Ensure Resource Optimisation	Manage the IT Management Framework	Manage Risk	Manage Security	Manage Assets	Manage Operations	Manage Service Requests and Incidents	Manage Problems	Manage Security Services	Manage Business Process Controls	Monitor, Evaluate and Assess Compliance With External Requirements
7.5	✓	✓	✓	✓	✓	✓		✓			✓	✓	
7.6	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓	
7.7	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
7.8	✓	✓	✓	✓	✓	✓					✓	✓	

	Evaluate, Direct and Monitor			**Align, Plan and Organise**			**Build, Acquire and Implement**	**Deliver, Service and Support**					**Monitor, Evaluate and Assess**
Risk	EDM 01	EDM 03	EDM 04	APO 01	APO 12	APO 13	BAI 09	DSS0 1	DSS 02	DSS 03	DSS 05	DSS 06	MEA 03
	Ensure Governance Framework Setting and Maintenance	Ensure Risk Optimisation	Ensure Resource Optimisation	Manage the IT Management Framework	Manage Risk	Manage Security	Manage Assets	Manage Operations	Manage Service Requests and Incidents	Manage Problems	Manage Security Services	Manage Business Process Controls	Monitor, Evaluate and Assess Compliance With External Requirements
8.1	✓	✓		✓	✓	✓					✓	✓	
8.2	✓	✓		✓	✓	✓					✓	✓	

✓ = Indicates that the process is mapped to the risk identified.

Based on the mapping process conducted in table 4 it is clear that the COBIT 5 framework can be used to identify controls which the organisation can deploy to reduce risks to an acceptable level.

CHAPTER 5: FINDINGS ON THE INCREMENTAL INFORMATION TECHNOLOGY STRATEGIC AND OPERATIONAL RISKS WHICH ARISE WHEN AN ORGANISATION ADOPTS A BYOD PROGRAM

Table 5 identifies possible safeguards which the organisation can deploy to reduce the risks identified in table 3 to an acceptable level.

Table 5

Number	Summarised risk identified	COBIT 5 reference	Possible safeguard or control from the literature reviewed or COBIT 5
1.1	Deployment of malware into organisations system.	EDM01, EDM03, APO01, APO12, APO13, DSS05.	a) The organisation should have a policy stating that mobile device users are only able to connect to the network if they have installed anti-malware software. b) The anti-malware software should be updated on a regular basis.
1.2	Malicious software targets smartphones and tablets.	EDM01, EDM03, APO01, APO12, APO13, DSS05.	a) The organisation should have a policy stating that mobile device users are only able to connect to the network if they have installed anti-malware software. b) The anti-malware software should be updated on a regular basis. c) Employees should be educated about what impact malware could have on the organisations sensitive data as well as the manner in which malware infiltrates the device.

Number	Summarised risk identified	COBIT 5 reference	Possible safeguard or control from the literature reviewed or COBIT 5
1.3	Hackers ability to control computer systems.	EDM01, EDM03, APO01, APO12, APO13, DSS05.	a) The organisation should encrypt their data. b) The organisation should have strong authentication methods in place to access the network. An example of this will include the use of tokens. c) Unauthorised devices which have been detected by the network access control software should block these devices immediately.
1.4	Data stolen or damaged.	EDM01, EDM03, APO01, APO12, APO13, DSS05.	a) The organisation should encrypt their data. b) The organisation should have strong authentication methods in place to access the network. An example of this will include the use of tokens.
1.5	Device disabled.	EDM01, EDM03, APO01, APO12, APO13, DSS05.	a) The organisation should have a policy stating that mobile device users are only able to connect to the network if they have installed anti-malware software. b) The anti-malware software should be updated on a regular basis. c) Employees should be educated about what impact malware could have on the organisations sensitive data as well as the manner in which malware infiltrates the device.

Number	Summarised risk identified	COBIT 5 reference	Possible safeguard or control from the literature reviewed or COBIT 5
1.6	Use of unapproved applications.	EDM01, EDM03, APO01, APO12, APO13, DSS05.	a) The organisation needs to have a policy stating which applications employees are permitted to download onto their devices. The policy should be updated on a regular basis to take into account the new malicious applications that has been brought to the attention of the IT department. b) The organisation could have a policy where they do spot checks on the mobile devices used by their employees. Where unapproved applications have been identified, the owner of the device should be requested to delete the application immediately.
2.1	Data leakage is a greater problem that Malware	EDM01, EDM03, APO01, APO12, APO13, DSS05.	a) Employees should be educated about the impact that data leakage could have on the organisation and how it occurs.
2.2	Employees sync mobile device with infected home computer.	EDM01, EDM03, APO01, APO12, APO13, DSS05.	a) Employees should be educated about the risks involved with syncing their mobile device with their home computer. b) The employee should be advised to run their anti-virus software on a regular basis.
2.3		EDM01, EDM03, APO01, APO12, APO13, DSS05.	a) The organisation should invest in on-device containerisation technology. b) The organisation should consider making use of a virtual desktop environment.

Number	Summarised risk identified	COBIT 5 reference	Possible safeguard or control from the literature reviewed or COBIT 5
			c) The organisations data stored on the device should be encrypted.
2.4	Loss of control over data stored in the Cloud.	EDM01, EDM03, APO01, APO12, APO13, DSS05.	a) The organisation should provide employees with a convenient method of securely sharing documents and collaborating on mobile devices.
2.5	Unauthorised access to sensitive data.	EDM01, EDM03, APO01, APO12, APO13, DSS05.	a) The organisations data which has been stored on the device should be encrypted. b) Employees should be educated about the risks involved with storing confidential data in the Cloud.
2.6	Potential outflow of finances as a result of data breach.	EDM01, EDM03, APO01, APO12, APO13, DSS05.	a) The organisation should have sufficient insurance to cover any financial outflows that arise as a result of a data breach.
3.1	Lost mobile devices create a security threat.	EDM01, EDM03, APO01, APO12, APO13, DSS05.	a) The organisations data which has been stored on the device should be encrypted. b) The organisation can make use of remote wiping facilities to delete all organisation related information that is stored on the device.
3.2	Criminals may gain access to confidential information.	EDM01, EDM03, APO01, APO12, APO13, DSS05.	a) The organisations data which has been stored on the device should be encrypted. b) The organisation can make use of remote wiping facilities to delete all organisation related information that is stored on the device.

Number	Summarised risk identified	COBIT 5 reference	Possible safeguard or control from the literature reviewed or COBIT 5
3.3	Information may not be password protected.	EDM01, EDM03, APO01, APO12, APO13, DSS05.	a) Employees should be educated about the advantages and disadvantages of not having a secure password on their mobile device. b) The organisation could have a policy where they do spot checks on the mobile devices used by their employees. Where mobile devices are identified with no password or a weak password, employees should be requested to create a password or change their password immediately.
3.4	Data may not be encrypted.	EDM01, EDM03, APO01, APO12, APO13, DSS05.	a) The organisation should have a policy that all data transmitted to employee's mobile devices should be encrypted at all times.
3.5	Mobile devices are easily stolen as a result of size.	EDM01, EDM03, APO01, APO12, APO13, DSS05.	a) Employees should be encouraged to be mindful of the whereabouts of the mobile devices at all times. b) Mobile device tracking facilities could be used to locate the mobile device. c) The organisation can make use of remote wiping facilities to delete all organisation related information that is stored on the device.
3.6	Data on mobile device which has been lost or stolen may be compromised.	EDM01, EDM03, APO01, APO12, APO13, DSS05, DSS06, MEA03.	a) The organisations data which has been stored on the device should be encrypted.

Number	Summarised risk identified	COBIT 5 reference	Possible safeguard or control from the literature reviewed or COBIT 5
3.7	Lost or stolen mobile devices may have personally identifying and confidential client information on it.	EDM01, EDM03, APO01, APO12, APO13, DSS05, DSS06, MEA03.	a) The organisations data which has been stored on the device should be encrypted. b) The organisation can make use of remote wiping facilities to delete all organisation related information that is stored on the device. c) The organisation should have sufficient insurance to cover possible law suits as a result of confidential information relating to their clients be revealed.
3.8	Organisation cannot remotely wipe lost mobile device.	EDM01, EDM03, APO01, APO12, APO13, DSS05, DSS06, MEA03.	a) The organisations data which has been stored on the device should be encrypted. b) The organisation should invest in software that will enable them to remotely wipe sensitive data off an employee's mobile device which has been lost or stolen.
3.9	Employees don't know what to do when device is lost or stolen.	EDM01, EDM03, APO01, APO12, APO13, DSS05, DSS06, MEA03.	a) The organisation should have a policy informing employees what they need to do in the event that their mobile device is lost or stolen.
4.1	Bluetooth device may be discoverable.	EDM01, EDM03, APO01, APO12, APO13, DSS05.	a) Employees should be educated about the risks involved with leaving their mobile devices on discoverable mode.

Number	Summarised risk identified	COBIT 5 reference	Possible safeguard or control from the literature reviewed or COBIT 5
4.2	Unauthorised data downloads.	EDM01, EDM03, APO01, APO12, APO13, DSS05.	a) The organisations data which has been stored on the device should be encrypted. b) The organisation should make use of network access control technology. Any unauthenticated device should be immediately blocked. c) Employees should be educated about the risks involved with leaving their mobile devices on discoverable mode as well as the risks involved with tethering.
4.3	Non-authenticated devices connecting to network.	EDM01, EDM03, APO01, APO12, APO13, DSS05	a) The organisation should make use of network access control technology. Any unauthenticated device should be immediately blocked.
4.4	Bluetooth and Wi-Fi technology are easily infected.	EDM01, EDM03, APO01, APO12, APO13, DSS05.	a) The organisation should make use of network access control technology. Any unauthenticated device should be immediately blocked. b) Anti-malware software should be loaded onto the mobile devices.
4.5	Data transmitted may be compromised.	EDM01, EDM03, APO01, APO12, APO13, DSS05.	a) The organisations data which has been stored on the device should be encrypted to prevent it from being compromised.

Number	Summarised risk identified	COBIT 5 reference	Possible safeguard or control from the literature reviewed or COBIT 5
5.1	Applications downloaded may steal or damage data.	EDM01, EDM03, APO01, APO12, APO13, DSS05	a) Employees should be educated about the risks involved with downloading applications onto their mobile devices. b) The organisations data which has been stored on the device should be encrypted.
5.2	Unapproved applications may be stored on mobile devices.	EDM01, EDM03, APO01, APO12, APO13, DSS05, DSS06.	a) The organisation should have a policy indicating which applications employees are permitted to download onto their devices.
5.3	Unapproved applications may not be easily detectable.	EDM01, EDM03, APO01, APO12, APO13, DSS05, DSS06.	a) The organisation could have a policy where they do spot checks on the mobile devices to identify whether or not the employee has any unapproved applications on their mobile device. Where mobile devices are identified with unapproved applications stored on it, employees should be requested to delete the application immediately.
5.4	Employees unaware of risky apps.	EDM01, EDM03, APO01, APO12, APO13, DSS05, DSS06.	a) The organisation should have a policy where the IT department sends out regular email communication to employees about which popular applications are risky as well as what the potential consequences are if they download one of these applications.

Number	Summarised risk identified	COBIT 5 reference	Possible safeguard or control from the literature reviewed or COBIT 5
6.1	Organisation may not be complying with laws and regulations.	EDM01, EDM03, APO01, APO12, APO13, DSS05, DSS06, MEA03.	a) The organisation should have a compliance officer who identifies which laws and regulations affect the organisation.
6.2	Organisation may be unaware of specific geographical laws and regulations.	EDM01, EDM03, APO01, APO12, APO13, DSS05, DSS06, MEA03.	a) The organisation should have a compliance officer who identifies which laws and regulations affect the organisation.
6.3	Communication laws may be violated.	EDM01, EDM03, APO01, APO12, APO13, DSS05, DSS06, MEA03.	a) The organisation should inform their employees which laws and regulations affect the organisation (including communication laws).
6.4	Organisations may not be able to ensure compliance on employee owned devices.	EDM01, EDM03, APO01, APO12, APO13, DSS05, DSS06, MEA03.	a) The organisation should have a compliance officer who identifies which laws and regulations affect the organisation. b) The organisation could have the employees sign a contract indicating that if they intentionally violate a law or regulation that they should have been knowledgeable, that they take personal responsibility for the non-compliance.

Number	Summarised risk identified	COBIT 5 reference	Possible safeguard or control from the literature reviewed or COBIT 5
6.5	Personal use software may be used for business purposes.	EDM01, EDM03, APO01, APO12, APO13, DSS05, DSS06, MEA03.	a) Employees should be informed that they should inspect the software license on their device to identify whether or not it is personal use software prior to using the software for business purposes. b) The organisation could have a policy where an employee needs to get the mobile device pre-approved prior to being allowed to use it to access the organisations sensitive data. Software licenses could be checked by the IT department at this point in time.
6.6	Organisations may be liable for additional costs where software licenses have been breached.	EDM01, EDM03, APO01, APO12, APO13, DSS05, DSS06, MEA03.	a) The organisation could have a policy where an employee needs to get the mobile device pre-approved prior to being allowed to use it to access the organisations sensitive data. Software licenses could be checked by the IT department at this point in time. b) The organisation should have sufficient insurance to cover themselves in the event that they are found to have breached a software licensing agreement.

Number	Summarised risk identified	COBIT 5 reference	Possible safeguard or control from the literature reviewed or COBIT 5
7.1	IT may not be able to manage all mobile devices.	EDM01, EDM03, EDM04, APO01, APO12, APO13, BAI09, DSS01, DSS02, DSS03, DSS05, DSS06.	a) The organisation my establish user self-support and third-party support options. b) The organisation may re-train existing service desk staff, and augment the mobile support team as needed. c) The organisation may make use of internal wikis, user forums, email distribution lists, enterprise social networking and other collaboration tools for user self-support.
7.2	IT may not be able to secure all mobile devices.	EDM01, EDM03, EDM04, APO01, APO12, APO13, BAI09, DSS01, DSS05, DSS06.	a) The organisation should implement a mobile device management system to reduce the risks associated with not being able to secure all mobile devices.
7.3	IT may not be able to successfully implement mobile security.	EDM01, EDM03, EDM04, APO01, APO12, APO13, BAI09, DSS01, DSS05, DSS06.	a) The organisation may make use of a network access controls systems to reduce the risk of anauthorised devices connecting to the network. b) The organisation should implement a mobile device management system to reduce the risks associated with not being able to secure all mobile devices.
7.4	Employees may select a device without considering IT support.	EDM01, EDM03, EDM04, APO01, APO12, APO13, DSS01, DSS05, DSS06.	a) The organisation could have a policy indicating which mobile devices they will support.

Number	Summarised risk identified	COBIT 5 reference	Possible safeguard or control from the literature reviewed or COBIT 5
7.5	Employee mobile devices may not be configured or locked down.	EDM01, EDM03, EDM04, APO01, APO12, APO13, DSS01, DSS05, DSS06.	a) The organisation should implement a mobile device management system to ensure that all mobile devices have been configured correctly.
7.6	IT may not pre-approve all mobile devices.	EDM01, EDM03, EDM04, APO01, APO12, APO13, BAI09, DSS01, DSS05, DSS06.	a) The organisation should have a policy whereby they only permit pre-approved mobile devices to connect to the organisations network.
7.7	IT may not be able to provide same level of support to all mobile devices.	EDM01, EDM03, EDM04, APO01, APO12, APO13, BAI09, DSS01, DSS02, DSS03, DSS05, DSS06.	a) The organisation my establish user self-support and third-party support options. b) The organisation may re-train existing service desk staff, and augment the mobile support team as needed. c) The organisation may make use of internal wikis, user forums, email distribution lists, enterprise social networking and other collaboration tools for user self-support.
7.8	The organisation may have open ports for employee owned.	EDM01, EDM03, EDM04, APO01, APO12, APO13, DSS05, DSS06.	a) The organisation should not have open ports. Employees should use some form of log on password to gain access to the network.

Number	Summarised risk identified	COBIT 5 reference	Possible safeguard or control from the literature reviewed or COBIT 5
8.1	Mobile device life cycle may shorten.	EDM01, EDM03, EDM04, APO01, APO12, APO13, DSS05, DSS06.	a) The organisation may re-train existing service desk staff, and augment the mobile support team as needed. b) Employees should be encouraged to keep their mobile phones for the duration of their mobile phone contracts.
8.2	Mobile devices may have planned obsolescence built into them.	EDM01, EDM03, EDM04, APO01, APO12, APO13, DSS05, DSS06.	b) Employees should be encouraged to keep their mobile phones for the duration of their mobile phone contracts.

The controls have been identified using the COBIT 5 framework and the literature review as a basis in identifying the controls. All other controls noted are purely incidental.

CHAPTER 6: CONCLUSION AND FURTHER RESEARCH

6.1 Conclusion

The aim of the research was to identify the incremental risks which arise as a result of an organisation adopting a BYOD program as well as using a recognised framework to identify controls which could be implemented to reduce the incremental risks to an acceptable level.

The study conducted revealed 50 incremental risks which could arise if an organisation adopts a BYOD program. The user of this research should note that there may be other incremental risks which may arise at their organisation. This is entirely dependent on the circumstances and control environment found at the organisation.

The research concluded that the COBIT 5 framework was an acceptable framework to use in identifying controls which could reduce the incremental risks to an acceptable level.

The incremental risks identified were mapped against the COBIT 5 framework.

The findings of the mapping exercise and the extensive literature review were used to identify potential safeguards which an organisation can employ in order to reduce the incremental risks to an acceptable level.

6.2 Future research

Possible future research could involve conducting a case study on a large South African organisation a few years down the line to see what impact the BYOD phenomenon has had on the organisation.

REFERENCES

ABI Research, 2013. *Transforming Your Organisation With Mobility,* Oyster Bay: ABI Research.

Accellion Inc., 2012. *BYOD File Sharing – Go Private Cloud to Mitigate Data Risks,* Palo Alto: s.n.

Anderson, N., 2013. *Cisco Bring Your Own Device - Device Freedom Without Compromising the IT Network,* s.l.: CISCO.

App Authority, 2013. *App Reputation Report,* Sanfrancisco: s.n.

ARUBA Networks, 2012. *Conquering today's bring-your-own-device challenges - A framework for successful BYOD initiatives,* Sunnyvale: s.n.

Bouchard, M., 2012. *A 3-STEP PLAN FOR MOBILE SECURITY,* s.l.: WEBSENSE.

BRI12, 2012. *BRING YOUR OWN DEVICE,* s.l.: ITNOW.

Burt, J., 2011. *BYOD Trend Pressures Corporate Networks,* s.l.: eWeek.

Cearley, D; Claunch, C., 2013. *The Top 10 Strategic Technology Trends for 2013,* s.l.: Gartner.

CISCO, 2012. *The Cisco BYOD Smart Solution,* s.l.: s.n.

CISCO, 2013. *Cisco Connected World—International Mobile Security: Survey Research Highlights and Considerations for Enterprise IT,* s.l.: s.n.

CITRIX, 2012. *Best practices to make BYOD simple and secure,* s.l.: s.n.

Costello, T. & Prohaska, B., 2013. *2013 Trends and Strategies,* s.l.: IT Pro.

DAT, 2012. *DATA SECURITY BYOD Security Risks On The Rise,* s.l.: INFORMATION MANAGEMENT.

Deloitte, 2013. *Understanding the Bring Your Own Device Landscape,* s.l.: s.n.

Dimitriadis, C., Lobel, M., Meyers, A. & Nedelchev, N., 2010. *Securing Mobile Devices,* Rolling Meadows: ISACA.

Drew, J., 2012. Managing Cybersecurity Risks. *Journal of Accountancy,* Volume August 2012, pp. 44-48.

Entner, R., 2011. *INTERNATIONAL COMPARISONS: THE HANDSET REPLACEMENT CYCLE,* s.l.: Recon Analytics.

Evangelista, M., 2013. *The Total Economic Impact of IBM Managed Mobility For BYOD,* s.l.: Forrester.

Fiering, L., 2013. *BYOD Doesn't Have to Be All or Nothing Match Smartphone, Tablet and PC Rollouts to Organizational Readiness and Employee Demand,* s.l.: Gartner.

Frances O'Brien, 16 April 2013. *Cut the Software Compliance Risks of BYOD,* s.l.: Gartner.

Gatewood, B., 2012. *THE NUTS AND BOLTS OF MAKING BYOD WORK,* s.l.: INFORMATION MANAGEMENT.

Good Technology, 2011. *Bring Your Own Devices Best Practices Guide - A Practical Guide for Implementing BYOD Programs at Your Organization,* s.l.: s.n.

Gupta, A; Milanes, C; Cozza, R; Lu, CK., 2013. *Market Share Analysis: Mobile Phones, Worldwide, 2Q13,* s.l.: Gartner.

Gupta, M., 2012. *COBIT 5 for Information Security.* s.l.:ISACA.

Hawkins, N. et al , 2012. *Bring Your Own Device & Consumerisation of IT.* s.l.:IBM.

IBM, 2011. *The New Workplace: Supporting "Bring your own",* s.l.: IBM.

IBM, 2012. *Securing end-user mobile devices in the enterprise,* s.l.: s.n.

Institute of directors of Southern Africa, 2009. *King Code of Governance for South Africa 2009,* s.l.: Institute of directors of Southern Africa.

ISACA , 2012a. *COBIT 5 Enabling Processes,* s.l.: s.n.

ISACA, 2007. *COBIT 4.1,* s.l.: ISACA.

ISACA, 2012b. *COBIT 5 Essential facts,* s.l.: s.n.

ISACA, 2012c. *COBIT 5 Framework,* s.l.: s.n.

ISACA, 2012. *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT,* Rolling Meadows: ISACA.

ISACA, 2012d. *COBIT 5 Implementation,* s.l.: s.n.

IT Governance Institute (ITGI), 2007. *COBIT 4.1,* s.l.: IT Governance Institute (ITGI).

Jaine, A., Shandag, D. & Upstreme., Sept - Oct 2012. Addressing Security and Privacy Risks in Mobile Applications. *IT Professional,* Volume 14, pp. 28, 33.

Kanaracus, C., 2012. *IBM CIO Embraces,* s.l.: COMPUTER WORLD.

Kaspersky, 2012. *SECURITY TECHNOLOGIES FOR MOBILE AND BYOD.,* s.l.: s.n.

Keeble, D., 2013. *THE CULTURE OF PLANNED OBSOLESCENCE IN TECHNOLOGY COMPANIES,* s.l.: OULO UNIVERSITY OF APPLIED SCIENCES.

Klossner, J., 2012. *CONSUMERIZATION OF IT - BYOD Is Driving IT 'Crazy,' Says Gartner,* s.l.: COMPUTERWORLD.

KONY, 2012a. *Harnessing BYOD Phenomenon – an IT Guide,* s.l.: s.n.

KONY, 2012b. *Write Once, Run Everywhere Mobile Technology,* s.l.: s.n.

Lennon, R. G., 2012. *Bring your own device (BYOD) with Cloud 4 education.* New York, USA, Splash.

Leong, K., 2013. *How to secure IT infrastructure with effective controls, compliance,* s.l.: Network World Asia.

Lung Kao, I., 2011. *Securing mobile devices in the business environment,* s.l.: IBM.

Mansfield-Devine, S., 2012. *BYOD and the enterprise network,* s.l.: Computer Fraud and Security.

Markelj, B. & Bernik, I., 2012. Mobile Devices amd Corporate Data Security. *International Journal of Education and Information Technologies,* 6(1), pp. 97-104.

Maycroft, N., 2009. *Consumption, planned obsolescence and waste.* s.l.:University of Lincoln.

McNally, J., 2013. *The 2013 COSO Framework & SOX Compliance,* s.l.: STRATEGIC FINANCE.

McQuire, N., 2012. *Global BYOD Attitudes and Best Practise for Multinational Organisations,* s.l.: IDC.

Mearian, L., 2012. *BYOD Exposes Perils,* s.l.: COMPUTERWORLD.

Miller, K., Voas, J. & Hurburt, G., 2012. *BYOD: Security and Privacy Considerations,* s.l.: IT Pro.

Miller, K., Voas, J. & Hurburt, G., Sept - Oct 2012. BYOD:Security and Privacy Considerations. *IT Professional,* 14(5), pp. 53-55.

Moore, C; Warner, J., 2012. *Industry Contexts And Constraints Diversify Approaches To Bring-Your-Own-Technology,* s.l.: Gartner.

Ng, V., 2011. *2012: The Impact of IT Convergance and Consumerization,* s.l.: Network World Asia.

O'Brien, F., 2013. *Cut the Software Compliance Risks of BYOD,* s.l.: Gartner.

Pelino, M., 2012. *Building The Case For A Bring-Your-Own-Device (BYOD) Program,* Cambridge: Forrester.

Ponemon Institute LLC, 2012. *Global Study on Mobility Risks,* s.l.: s.n.

Rohan, 2013. *Bring-Your-Own-Device (BYOD) Market Poise $181.39 Billion by 2017.* [Online]
Available at: http://www.sbwire.com/press-releases/bring-your-own-device-byod-market-poise-18139-billion-by-2017-321838.htm
[Accessed 26 September 2013 September 2013].

Rose, C., 2012. BYOD: An Examination Of Bring Your Own Device In Business. *The Clute Institute,* 17(2), pp. 65 - 70.

Rouse, M., 2010. *Whatif.com.* [Online]
Available at: http://searchcloudcomputing.techtarget.com/definition/cloud-computing
[Accessed 31 October 2013].

Rouse, M., 2011. *Whatis.com.* [Online]
Available at: http://searchcompliance.techtarget.com/definition/control-framework
[Accessed 17 October 2013 2013].

Shanbhag, A. & Kumar, A., 2012. *Addressing Security and Privacy Risks in Mobile Applications,* s.l.: Tata Consulting Services.

Simpson, B., 2012. *BRING YOUR OWN DEVICE?.* [Online]
Available at: http://www.pirean.com/industry-insight/blogs/bring-your-own-device/
[Accessed 26 September 2013 September 2013].

Staut, M., 2012. *BYOD: A revolution on the rise - Bring Your Own Device' is poised to expand.* [Online]
Available at:
http://www.cpa2biz.com/Content/media/PRODUCER_CONTENT/Newsletters/Articles_2012/CPA/Apr/RevolutionRise.jsp
[Accessed 26 September 2013 September 2013].

Stroud, R., 2012. *5 Essential facts about COBIT 5,* s.l.: ISACA.

Tibken, S., 2012. *CNet.* [Online]
Available at: http://news.cnet.com/8301-1035_3-57542502-94/google-ties-apple-with-700000-android-apps/
[Accessed 26 September 2013 September 2013].

Treadway Commission, 2013. *Internal integrated framework (COSO),* s.l.: s.n.

Vining, J., 2013. *Best Practices for Government BYOD Legal Discovery Requests,* s.l.: Gartner.

Vining, J; Pescatore, J; Girard, J., 2012. *For Better Decisions About Costs and Benefits,BYOD Pilots and Policies Need Clarity,* s.l.: Gartner.

VIOUNO, B., 2012. *As mobile devices continue to flood the enterprise, IT leaders grapple with ways to manage the risks,* s.l.: COMPUTERWORLD.

Vodafone, 2012. *Bring your own device: a considered approach,* s.l.: s.n.

Willis, D., 2013a. *Bring Your Own Device Program Best Practises (BYOD).* s.l.:Gartner.

Willis, D., 2013b. *Bring Your Own Device: The Facts and the Future,* s.l.: Gartner.

Yongqing, G. & Dan, S., 2011. *A smart phone anti-theft solution based on locking card of mobile phone.* Chengdu , China, Computational and Information Sciences (ICCIS).